Mittelstand-Digital
Zentrum
Handel

INFO
BLATT

Rechtliche Rahmenbedingungen der KI-Nutzung

Der Einsatz von Künstlicher Intelligenz (KI) wird in Zukunft eine immer wichtigere Rolle spielen. Um das Vertrauen in diese Technologie zu stärken, sind eindeutige und transparente Regeln notwendig.

Der AI Act – Rechtsrahmen für KI in der EU

Am 21. Mai 2024 hat der Rat der 27 EU-Mitgliedstaaten die KI-Verordnung (Verordnung (EU) 2024/1689, „AI Act“) verabschiedet und damit einen einheitlichen Rechtsrahmen für den Einsatz Künstlicher Intelligenz in der Europäischen Union geschaffen. Die Verordnung trat offiziell am 1. August 2024 in Kraft. Laut Artikel 113 gelten ihre Bestimmungen größtenteils ab dem 2. August 2026, einige Regelungen bereits ab dem 2. Februar 2025 bzw. ab dem 2. August 2025 und weitere ab dem 2. August 2027.

Dieses Infoblatt begleitet Unternehmen dabei, Künstliche Intelligenz rechtskonform und verantwortungsvoll einzusetzen. Es fasst die wesentlichen Vorgaben des europäischen Rechtsrahmens kompakt zusammen und bietet eine praxisnahe Orientierung.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Zeitleiste des AI Acts

02.02.2025

Februar 2025: KI-Systeme, die ein unannehmbares Risiko darstellen, sind verboten und dürfen nicht mehr eingesetzt werden (vgl. Abschnitt „Risikokategorien für KI-Systeme“).

Anbieter und Betreiber sind verpflichtet, sicherzustellen, dass Mitarbeitende, die mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ausreichende Kompetenzen verfügen (vgl. Abschnitt „KI-Kompetenzen im Unternehmen“).

02.08.2025

August 2025: Anwendbarkeit der Bestimmungen für KI-Systeme mit „allgemeinem Verwendungszweck“.

Beispiel: *Unternehmen, die große Sprachmodelle wie ChatGPT oder Bildgeneratoren wie DALL-E entwickeln oder nutzen, müssen ab diesem Zeitpunkt sicherstellen, dass sie transparent über ihre Funktionsweise informieren und potenzielle Risiken minimieren.*

02.08.2026

August 2026: Allgemeine Anwendbarkeit der KI-Verordnung für Unternehmen und Behörden.

02.08.2027

August 2027: Anwendbarkeit der KI-Verordnung für bestimmte Hochrisikosysteme, die besonders strengen Anforderungen unterliegen.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Risikokategorien für KI-Systeme

Die KI-Verordnung definiert **vier Risikokategorien** für KI-Systeme, für die unterschiedlich strenge Bestimmungen gelten:

1. Unannehmbares Risiko (Verboten seit dem 02.02.2025):

KI-Systeme, die als unvertretbares Risiko für die Sicherheit, die Grundrechte oder die demokratischen Werte angesehen werden. So ist z. B. das Social Scoring durch Behörden (nach dem Vorbild Chinas), d. h. das Bewerten oder Einstufen von Individuen basierend auf ihrem Verhalten, wirtschaftlichem Status oder persönlichen Merkmalen durch Behörden verboten. Grund: Dies könnte zur Diskriminierung und ungerechtfertigter Benachteiligung führen.

2. Hohes Risiko (Strenge Regulierung):

Diese Kategorie umfasst KI-Systeme, die in sensiblen Bereichen eingesetzt werden und erhebliche Auswirkungen auf die Sicherheit, Rechte oder den Alltag der Bürger:innen haben können.

Beispiele:

- **KI im Personalwesen** (z. B. automatisierte Auswahl von Bewerberbenden – hier besteht das Risiko, dass die KI diskriminierende Tendenzen aufweisen könnte, z. B. unfaire Benachteiligung aufgrund von Geschlecht, Alter oder Herkunft).
- **KI in der Finanzbranche** (z. B. Kreditwürdigkeitsprüfung – unfaire oder intransparente Bewertungen könnten dazu führen, dass Menschen von wichtigen finanziellen Dienstleistungen ausgeschlossen werden).

Diese Systeme müssen umfassende Transparenz- und Sicherheitsanforderungen erfüllen. So müssen Unternehmen dokumentieren, wie Risiken minimiert werden. Nutzer:innen müssen darüber informiert werden, dass sie mit einer KI interagieren und kritische Entscheidungen müssen durch Menschen überwacht werden können. Zudem müssen Unternehmen nachweisen, dass die zum Training der KI verwendeten Daten repräsentativ sind, um Verzerrungen und Benachteiligungen zu vermeiden.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

3. Begrenztes Risiko (Eingeschränkte Regulierung):

Bei KI-Systemen (z. B. Chatbots), die zwar gewisse Risiken bergen, aber diese auf ein moderates Maß beschränkt sind, greift ein reduzierter Regulierungsrahmen sowie eine Transparenzpflicht gegenüber den Nutzenden.

Beispiele:

- **Chatbots,** wie ChatGPT, Siri oder Alexa, die mit Kund:innen interagieren und Fragen beantworten oder Informationen bereitstellen - Nutzer:innen müssen darüber informiert werden, dass sie mit einer KI interagieren.
- **Empfehlungssysteme in Onlineshops** – Transparenz über die Funktionsweise der Empfehlung ist erforderlich (z. B. Kennzeichnung von personalisierten Inhalten).
- **KI-gestützte Text- oder Bildgenerierung** – KI, die Bilder oder Texte erstellt, wie DALL·E oder Midjourney - Inhalte sollten als KI-generiert gekennzeichnet werden, um Täuschung zu vermeiden.

4. Minimales Risiko (Frei nutzbar):

KI-Systeme mit geringem oder keinem Risiko, können ohne besondere Auflagen verwendet werden.

Beispiele:

- **Spam-Filter** als Modul eines E-Mail-Programms
- **Automatische Übersetzungstools** wie DeepL oder Google Translate

Solche Systeme sind kaum reguliert, müssen jedoch Datenschutzregeln einhalten.

Das Hauptziel der KI-Verordnung ist es, einen einheitlichen und sicheren Rechtsrahmen für die Entwicklung, den Einsatz und die Nutzung von Künstlicher Intelligenz innerhalb der Europäischen Union zu schaffen. Dabei sollen ethische Grundsätze gewahrt, Grundrechte geschützt und Innovationen gefördert werden.

Unternehmen sollten frühzeitig prüfen, in welche Risikokategorie ihre KI-Anwendungen fallen, um rechtzeitig alle regulatorischen Anforderungen erfüllen und zugleich die Chancen einer verantwortungsvollen KI-Nutzung optimal ausschöpfen zu können.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Welche Unternehmen/Organisationen sind von der KI-Verordnung betroffen?

Die KI-Verordnung gilt grundsätzlich für alle Unternehmen, die KI-Systeme entwickeln, bereitstellen oder **nutzen**, sofern diese in der EU angewendet werden, oder deren Ergebnisse Personen in der EU betreffen. Dies betrifft sowohl große Konzerne als auch kleine und mittlere Unternehmen (KMU), die KI-Technologien in ihre Produkte oder Dienstleistungen integrieren. Die private Nutzung von KI ist von der Verordnung ausgenommen.

Datenschutz

Beim Einsatz von KI sind Datenschutzgesetze einzuhalten, sofern personenbezogene verarbeitet werden. Besonders relevant sind hier die Vorschriften der Datenschutz-Grundverordnung (DSGVO).

1. Rechtmäßigkeit der Datenverarbeitung

Gemäß Art. 6 DSGVO ist für die Verarbeitung personenbezogener Daten eine gültige Rechtsgrundlage erforderlich. Mögliche Grundlagen sind die Einwilligung der betroffenen Person, die Erfüllung eines Vertrags oder berechtigte Interessen des Verantwortlichen.

Beispiel: *Ein E-Commerce-Unternehmen setzt KI-Algorithmen ein, um das Kaufverhalten seiner Kund:innen zu analysieren. Basierend auf früheren Einkäufen und Browsing-Daten zeigt das System personalisierte Werbeanzeigen und Produktempfehlungen. Hierbei muss der Nutzende vorher zustimmen, dass seine Daten für personalisierte Werbung genutzt werden dürfen.*

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

2. Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung sensibler Daten, wie etwa Gesundheitsdaten oder Daten zur ethnischen Herkunft, ist nach Art. 9 DSGVO grundsätzlich untersagt, es sei denn, es liegt eine ausdrückliche Einwilligung der betroffenen Person oder ein anderer Ausnahmefall (geregelt Art. 9 Abs. 2) vor.

Beispiel: *Eine KI, die Gesundheitsdaten auswertet, darf dies nur tun, wenn eine ausdrückliche Einwilligung der betroffenen Person vorliegt.*

3. Transparenz und Informationspflichten

Nach Art. 13 und 14 DSGVO müssen betroffene Personen über die Verarbeitung ihrer Daten informiert werden. Dies schließt Informationen über den Zweck der Verarbeitung, die Dauer der Speicherung, die Kategorien der verarbeiteten Daten und die Rechte (z. B. Recht auf Löschung) der Betroffenen ein.

4. Datenschutz-Folgenabschätzung (DSFA)

Wenn der Einsatz eines KI-Systems voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt, ist gemäß Art. 35 DSGVO eine DSFA durchzuführen. Dies betrifft insbesondere KI-Anwendungen, die automatisierte Entscheidungen mit erheblichen Auswirkungen auf die betroffenen Personen treffen.

Beispiel: *Eine Bank, die eine KI zur automatischen Kreditbewilligung nutzt, muss eine DSFA durchführen, da die Entscheidung erhebliche Auswirkungen auf Kund:innen hat.*

5. Prinzipien „Privacy by Design“ und „Privacy by Default“

Artikel 25 DSGVO verpflichtet Verantwortliche, Datenschutz bereits bei der Entwicklung („Privacy by Design“) und durch standardmäßig datenschutzfreundliche Einstellungen („Privacy by Default“) zu gewährleisten. Das bedeutet, dass technische und organisatorische Maßnahmen getroffen werden müssen, um den Schutz personenbezogener Daten sicherzustellen. Zudem dürfen nur die notwendigen Daten verarbeitet werden.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

6. Auftragsverarbeitung

Werden externe Dienstleister für die Entwicklung oder den Betrieb von KI-Systemen eingesetzt, ist gemäß Art. 28 DSGVO ein Auftragsverarbeitungsvertrag abzuschließen, der sicherstellt, dass der Dienstleister die Daten im Einklang mit den Datenschutzvorschriften verarbeitet.

7. Rechte der betroffenen Personen

Die DSGVO gewährt betroffenen Personen verschiedene Rechte, darunter das Recht auf Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17) und Widerspruch (Art. 21). Diese Rechte müssen auch im Kontext von KI-Anwendungen gewährleistet sein.

8. KI und Vertraulichkeit / Geheimnisschutz

Personenbezogenen Daten oder Firmengeheimnisse / vertrauliche Daten sollte man im Internet und ganz besonders bei der Verwendung von Künstlichen Intelligenzen ganz besonders schützen und nicht in öffentliche KI-Systeme eingeben. Daten, die in eine öffentliche KI eingespeist werden, kann man regelmäßig nicht mehr zu löschen oder berichtigen. Zudem lernen und trainieren die meisten (kostenlosen) KI-Systeme auch mit den eingegebenen bzw. hochgeladenen Daten, so dass hier größte Vorsicht geboten ist.
Beispiele:

- Unwiderrufliche Speicherung und Weiterverarbeitung von Daten - eine Person gibt aus Versehen ihre private Telefonnummer in ein KI-Tool ein. Falls die KI die Daten speichert, könnten sie später in generierten Antworten auftauchen.
- Missbrauch und Datenlecks - ein/eine Mitarbeiter:in gibt in einen KI-Chatbot Geschäftsgeheimnisse ein. Falls der Anbieter der KI die Daten speichert oder ein Cyberangriff erfolgt, könnten vertrauliche Informationen an die Öffentlichkeit gelangen.
- Vertrauliche Unternehmensstrategien - ein/eine Manager:in nutzt KI, um eine Strategie für ein neues Produkt zu analysieren. Falls die KI diese Informationen speichert, könnten Wettbewerber darauf zugreifen, wenn sie ähnliche Anfragen stellen.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

KI und Urheberrecht

Wenn mit KI Inhalte erstellt werden, gelten die Regelungen zum Urheberrecht. Das gilt auch für die Erhebung und die Nutzung von sogenannten Trainingsdaten im Rahmen des Lernens der KI.

1. Training von KI-Systemen:

Beim Training von KI-Anwendungen stellt sich die Frage, ob geschützte Inhalte für maschinelles Lernen vervielfältigt werden dürfen und Daten für Trainingszwecke benutzt werden dürfen. Gemäß § 44b II UrhG sind Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text und Data Mining zulässig. Das heißt, eine KI kann mit öffentlich zugänglichen Daten (z. B. Fotos) aus dem Internet trainiert werden.

Der Rechteinhaber kann dem Text- und Datamining seiner Werke, d. h. der Nutzung zum Training von KI zwar widersprechen, jedoch ist nach § 44b III UrhG ein Nutzungsvorbehalt bei online zugänglichen Werken nur dann wirksam, wenn er in maschinenlesbarer Form erfolgt. Wie dies genau technisch umzusetzen ist (z. B. Eintrag in robots.txt-Datei) ist aktuell noch umstritten.

Beispiel: *Eine KI wird mit Fotografien oder digitalen Kunstwerken trainiert, um neue Bilder im Stil bekannter Künstler:innen zu erstellen. Fotograf:innen oder Künstler:innen können eine Opt-out-Erklärung abgeben, um zu verhindern, dass ihre Werke für das KI-Training verwendet werden.*

2. Nutzung von KI-generierten Inhalten:

Nach derzeit herrschender Meinung sind Ergebnisse von KI-Systemen (KI generierter Inhalt) nicht urheberrechtlich geschützt, sondern für jedermann frei nutzbar. Dies führt insbesondere dann zu Problemen, wenn der durch KI generierte Inhalt (z. B. Fotos, Text, oder auch Softwarecode) an Dritte zur ausschließlichen Nutzung lizenziert werden soll.

Ob und inwieweit ein komplexer Prompt, d. h. die Eingabeaufforderung mit der ein von der KI generierter Inhalt erzeugt wird, urheberrechtlich geschützt ist, ist umstritten.

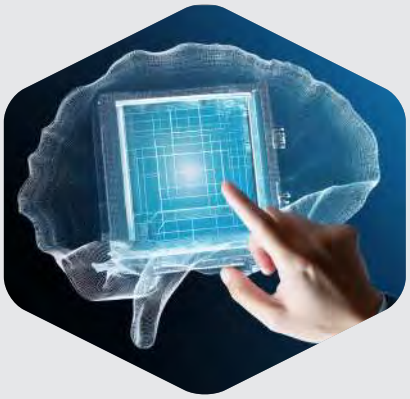
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Markenrecht

KI-Systeme können genutzt werden, um Logos, Markennamen oder Produktdesigns zu generieren. Dabei ist zu beachten, dass die durch KI erstellten Designs u.U. gegen bereits bestehende Marken oder Designs verstoßen können (Verwechslungsgefahr). Da KI-Modelle oft auf bestehenden Daten trainiert werden, besteht das Risiko, dass generierte Inhalte Elemente enthalten, die urheber- oder markenrechtlich (§14 Markengesetz) geschützt sind oder mit geschützten Marken verwechselt werden könnten. Es ist daher unerlässlich, vor der Nutzung solcher KI-generierten Designs eine gründliche Recherche durchzuführen, um mögliche Rechtsverletzungen zu vermeiden.

Beispiel: *Ein Start-up nutzt eine KI, um ein neues Logo für seine Marke zu erstellen. Das KI-generierte Logo weist starke Ähnlichkeiten mit dem Adidas-Logo (drei Streifen) auf. Falls das Logo zu nah am Original ist, könnte dies eine Markenrechtsverletzung darstellen.*

Transparenzpflichten



Neben den allgemeinen Transparenzpflichten aus der DSGVO gibt die KI-Verordnung (Artikel 50) weitere Anforderungen an die Transparenz vor, die ab dem 2. August 2026 gelten.

1. Transparenzpflichten bei der Nutzung von KI-generierten Inhalten:

Gemäß der KI-Verordnung müssen Inhalte, die durch generative KI-Systeme erstellt oder manipuliert wurden, klar als solche gekennzeichnet sein. Dies betrifft insbesondere sogenannte „Deepfakes“, bei denen Personen ohne deren Zustimmung dargestellt werden, als hätten sie bestimmte Handlungen vorgenommen oder Aussagen getroffen. In solchen Fällen ist es erforderlich, in angemessener, rechtzeitiger, klarer und sichtbarer Weise offenzulegen, dass der Inhalt künstlich generiert oder manipuliert wurde. Wenn möglich, sollte auch der Name der natürlichen oder juristischen Person genannt werden, die den Inhalt generiert oder manipuliert hat.

Beispiel: *Ein Onlineshop nutzt KI, um realistisch aussehende Produktbilder zu generieren, ohne, dass echte Fotos existieren. Der Shop muss kennzeichnen, dass die Bilder KI-generiert sind, z. B. durch einen Hinweis: „Dieses Bild wurde mit KI erstellt.“*

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

2. Transparenz bei der Nutzung von KI-Systemen:

Unternehmen, die KI-Systeme einsetzen, sind verpflichtet, Nutzer:innen darüber zu informieren, dass sie mit einer KI und nicht mit einem menschlichen Akteur interagieren. Dies gilt insbesondere für Chatbots oder virtuelle Assistenten.

Beispiel: *Ein Unternehmen nutzt einen KI-Chatbot, um Kundenanfragen automatisch zu beantworten. Nutzer:innen müssen sofort erkennen, dass er mit einer KI und nicht mit einem Menschen spricht.*

3. Anforderungen für Hochrisiko-KI-Systeme:

Artikel 13 der KI-Verordnung legt spezifische Transparenz- und Informationspflichten für Hochrisiko-KI-Systeme fest. Diese Anforderungen zielen darauf ab, sicherzustellen, dass der Betrieb solcher Systeme für die Anwendenden ausreichend transparent ist, sodass sie die Ergebnisse interpretieren und angemessen nutzen können. Dazu müssen Anbieter von Hochrisiko-KI-Systemen prägnante, vollständige und klare Betriebsanleitungen bereitstellen, die für die Anwendenden relevant, zugänglich und verständlich sind. Diese Anleitungen sollten mindestens Informationen über die Identität und Kontaktdaten des Anbieters, die Merkmale, Fähigkeiten und Leistungsgrenzen des Systems sowie Maßnahmen zur menschlichen Aufsicht enthalten.

Beispiel: *Eine Firma nutzt eine KI, die Bewerbungen automatisch nach Qualifikationen filtert. Die Bewerberbenden müssen darüber informiert werden, dass eine KI ihre Bewerbung geprüft hat und welche Kriterien verwendet wurden.*

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein *Whitepaper* veröffentlicht, das die Elemente von Transparenz in KI-Systemen definiert und erläutert.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Mittelstand-Digital Zentrum Handel

KI-Kompetenzen im Unternehmen

Seit dem 2. Februar 2025 sind Unternehmen, die unter die KI-Verordnung fallen, dazu verpflichtet, sicherzustellen, dass ihre Mitarbeitenden, die mit KI-Systemen arbeiten, über grundlegende Kenntnisse im Umgang mit Künstlicher Intelligenz verfügen.

1. Ermittlung des KI-Einsatzes im Unternehmen:

Unternehmen müssen alle aktuell genutzten KI-Systeme und deren spezifische Anwendungsbereiche identifizieren.

2. Bewertung des Schulungsbedarfs:

Zunächst müssen die vorhanden Kompetenzen der Mitarbeitenden in Bezug auf die genutzten KI-Systeme festgestellt werden. Anschließend muss der zusätzliche Schulungsbedarf bestimmt werden.

3. Schulung und Sensibilisierung

Auf Grundlage der Bedarfsanalyse sollten geeignete Schulungsmaßnahmen konzipiert oder bestehende Weiterbildungsangebote auf dem Markt ermittelt werden. Dazu gehören beispielsweise:

- **Grundlagen:** Einführung in Künstliche Intelligenz, deren Funktionsweise sowie Chancen und Risiken.
- **Fachspezifische Weiterbildungen:** Vertiefende Schulungen für spezifische Anwendungsbereiche, insbesondere in sicherheitskritischen oder branchenspezifischen Kontexten.
- **Regelmäßige Auffrischungskurse:** Zur Aktualisierung und Vertiefung vorhandener KI-Kenntnisse.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

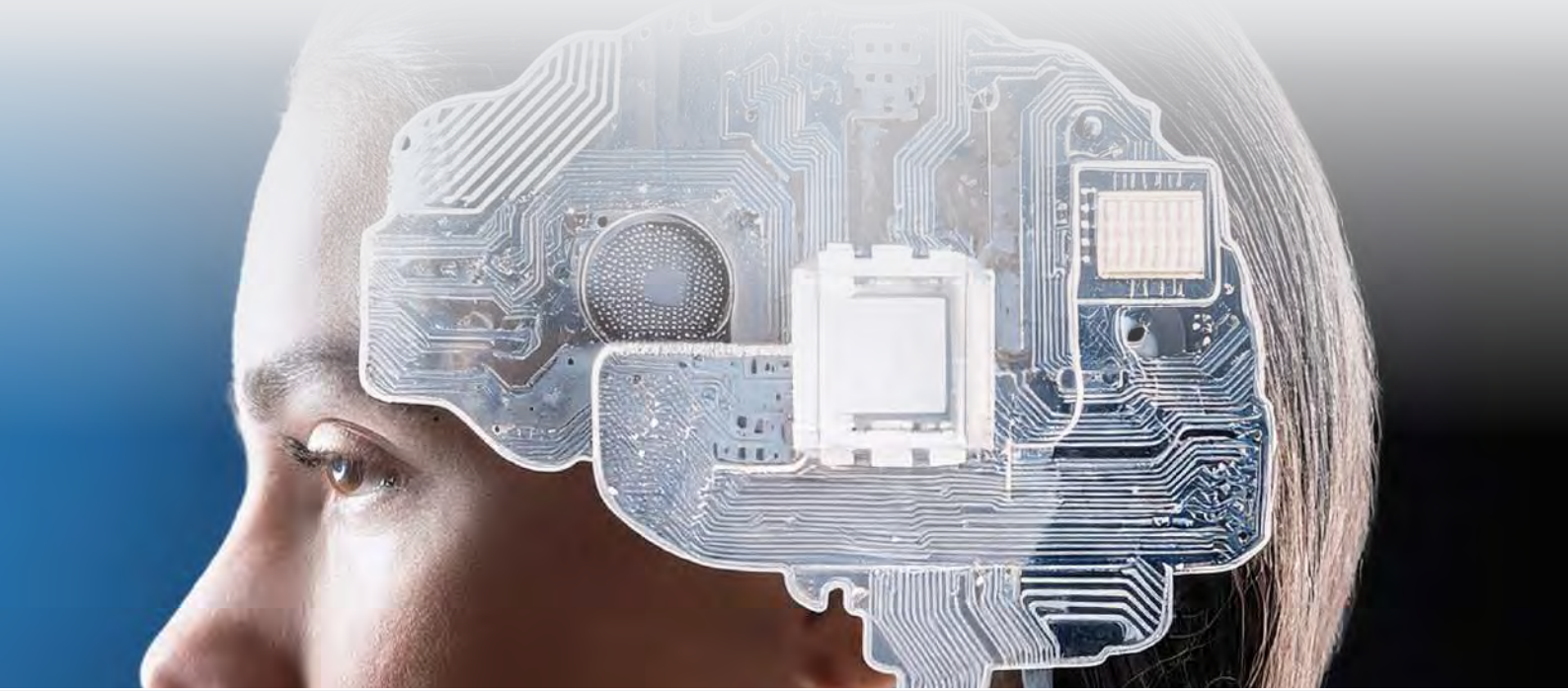
Unternehmen müssen mit den KI-Kompetenzschulungen sicherstellen, dass ihre Mitarbeitenden ausreichend geschult sind, um KI verantwortungsvoll und sicher zu nutzen. Mitarbeitende sollen dadurch in die Lage versetzt werden

- ein grundlegendes Verständnis von KI zu erwerben,
- die Funktionsweise der eingesetzten KI-Systeme zu verstehen,
- die Risiken und Grenzen von KI richtig einschätzen zu können,
- die regulatorischen Anforderungen der EU-KI-Verordnung zu kennen,
- KI-Entscheidungen zu überwachen und menschliche Kontrolle auszuüben.

Dies stärkt das Vertrauen in KI-Technologien, reduziert rechtliche Risiken und sorgt für eine ethische Nutzung im Arbeitsalltag. Falls ein Unternehmen dies nicht sicherstellt, drohen Sanktionen und erhebliche Bußgelder nach der KI-Verordnung.

4. Dokumentation

Obwohl der Artikel 4 der KI-Verordnung keine explizite Dokumentationspflicht vorschreibt, ist es für Unternehmen ratsam, die durchgeführten Schulungsmaßnahmen und die erworbenen Kompetenzen ihrer Mitarbeitenden gründlich zu dokumentieren. Eine solche Dokumentation dient als Nachweis der Erfüllung der gesetzlichen Anforderungen und kann im Falle von Überprüfungen durch Aufsichtsbehörden von entscheidender Bedeutung sein, um potenzielle Risiken zu reduzieren und die Haftung im Schadensfall zu begrenzen.



Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Sanktionen

Bei Nichteinhaltungen der geltenden Regeln besteht die Möglichkeit, dass auf Unternehmen hohe Geldstrafen zukommen. Diese können im Rahmen der DSGVO bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes des Unternehmens betragen. Unternehmen, die gegen die KI-Verordnung verstoßen, können mit noch erheblicheren Geldstrafen belegt werden:

- **Verstöße gegen verbotene KI-Praktiken:** bis zu 35 Millionen Euro oder 7 Prozent des weltweiten Jahresumsatzes
- **Verstöße gegen Hochrisiko-KI-Anforderungen:** bis zu 15 Millionen Euro oder 3 Prozent des Jahresumsatzes
- **Verstöße gegen Dokumentationspflichten:** bis zu 7,5 Millionen Euro oder 1,5 Prozent des Jahresumsatzes

Fazit

Die Regulierung durch die KI-Verordnung stellt Unternehmen vor neue Herausforderungen, schafft aber gleichzeitig eine notwendige Vertrauensbasis für den breiten Einsatz von KI in der Gesellschaft. Die Balance zwischen Innovation und Sicherheit steht im Mittelpunkt der neuen Vorschriften. Unternehmen sind nun in der Pflicht, ihre KI-Strategien an die rechtlichen Anforderungen anzupassen.

Vor allem KMU sollten die Veränderungen nicht als reine Belastung, sondern als Chance zur Optimierung ihrer Prozesse betrachten. Durch verantwortungsvollen Einsatz von KI, Schulung der Mitarbeitenden und Berücksichtigung von Datenschutz und ethischen Aspekten können Unternehmen nicht nur rechtliche Risiken minimieren, sondern auch Vertrauen bei Kunden, Partnern und der Öffentlichkeit stärken.

Insgesamt wird deutlich: **KI ist nicht nur eine Technologie, sondern eine Verantwortung**. Wer KI **ethisch, transparent und rechtskonform** einsetzt, wird langfristig von den Chancen dieser Technologie profitieren.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Quellen und weiterführende Informationen

1. **Verordnung (EU) 2024/1689 (KI-Verordnung)** https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689
2. **Verordnung (EU) 2016/679 (DSGVO)** https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679
3. **Richtlinie (EU) 2019/79 (Urheberrecht im digitalen Binnenmarkt)** https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0790
4. **Gesetz über Urheberrecht und verwandte Schutzrechte** https://www.gesetze-im-internet.de/urhg/
5. **Gesetz über den Schutz von Marken und sonstigen Kennzeichen** https://www.gesetze-im-internet.de/markeng/
6. **Bundesamt für Sicherheit in der Informationstechnik (BSI): „Transparenz von KI-Systemen“** https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Whitepaper-Transparenz-KI-Systeme.pdf?__blob=publicationFile&v=3
7. **bitkom „Umsetzungsleitfaden zur KI-Verordnung“** https://www.bitkom.org/sites/main/files/2024-10/241028-bitkom-umsetzungsleitfaden-ki.pdf

Das Mittelstand-Digital Zentrum Handel gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Infoblatt: Rechtliche Rahmenbedingungen der KI – 04 2025
Mittelstand-Digital Zentrum Handel

ibi research an der Universität Regensburg GmbH
Galgenbergstraße 25, 93053 Regensburg

digitalzentrumhandel.de

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital